Auditdienst Rijk
Ministerie van Financiën

Privacy audit Wpg 2015
Politie

Colofon

Titel	Privacy audit Wpg 2015 Politie
Datum	29 oktober 2015
Kenmerk	ADR 2015 1306

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

Assuranceverklaring

In 2014 heeft de heer D. Heerschop, lid Korpsleiding en CIO, de Auditdienst Rijk (ADR) van het ministerie van Financiën opdracht gegeven om over de jaren 2011 tot en met 2014 een privacy audit uit te voeren bij de politie op grond van de Wet politiegegevens (Wpg).
Deze privacy audit had tot doel op systematische wijze te toetsen of aan de bepalingen van de Wpg op adequate wijze uitvoering is gegeven ten aanzien van de in de wet genoemde verwerkingen.

Dit onderzoek is uitgevoerd conform de richtlijn 3600N, 'Assurance-opdrachten met betrekking tot de bescherming van persoonsgegevens (privacy audits) ' van juni 2006, van de NIVRA en de NOREA.

Op grond van onze werkzaamheden concluderen wij dat het stelsel van maatregelen en procedures gericht op de bescherming van de politiegegevens, betrekking hebbende op de in de Wpg genoemde artikelen, naar de stand van ultimo december 2014, in opzet, bestaan en werking niet of niet geheel heeft voldaan aan de vereisten zoals genoemd in de Wpg.

Het oordeel heeft betrekking op de zogenaamde verwerkingen genoemd in de Wpg. Het hierbij gehanteerde normenkader omvat de door de politie te nemen maatregelen. Tekortkomingen op deze vlakken hebben uiteindelijk geleid tot het geformuleerde oordeel.

De verantwoordelijke, zijnde de korpschef van de politie, de heer G. Bouman, is, op grond van artikel 4 lid 1 van de Regeling Periodieke Audit politiegegevens, verplicht binnen drie maanden een verbeterrapport op te stellen waarin de maatregelen worden beschreven die getroffen zijn ter verbetering van de in de privacy audit geconstateerde tekortkomingen. Op grond van artikel 4 lid 3 dient hercontrole plaats te vinden. Wij adviseren de hercontrole te laten uitvoeren door de interne auditors van de politie. De resultaten van het verbeterrapport en de uitgevoerde hercontrole zullen in de volgende privacy audit worden meegenomen.

Den Haag, d.d. 29 oktober 2015,

drs. D. van Ilpenhof RE CISA

Samenvatting

Over de jaren 2011 t/m 2014 hebben wij voor de tweede keer een privacy audit uitgevoerd bij de politie. Wij constateren dat de politie niet of niet geheel voldoet aan bij of krachtens de Wpg gestelde voorschriften.

De belangrijkste bevindingen die hebben geleid tot de conclusie in de assurance-verklaring, dat het stelsel van maatregelen en procedures gericht op de bescherming van de politiegegevens bij de politie niet of niet geheel heeft voldaan aan de vereisten zoals genoemd in de Wpg, zijn als volgt.

- De eenheden hebben de afgelopen periode werkzaamheden verricht in het kader van de implementatie van de Wpg binnen de politie. In vergelijking met de eerste privacy audit is mede door deze inspanningen de bewustwording over de Wpg binnen de politie groeiende en wordt het belang en nut van de Wpg vaker onderkend. Binnen het implementatieproject heeft men landelijke procedures opgezet voor een aantal risicovolle Wpg-onderwerpen. De implementatie van de landelijke procedures binnen de eenheden is echter nog niet geheel afgerond. Binnen de politie wordt momenteel nog een diversiteit aan werkwijzen gehanteerd.
- De Wpg wordt binnen de politie nog te veel gezien als een 'losstaand project', terwijl dit onderdeel uit zou moeten maken van alle politieprocessen. Tegelijkertijd ondersteunen de IT-systemen de gebruikers onvoldoende, waardoor onevenredig veel inspanning is vereist om buiten de systemen om, de Wpg-normen na te kunnen leven. Zo zijn in de IT-systemen de geautomatiseerde controles voor de Wpg niet ingebouwd en is het gegevensbeheer vaak niet op orde.
- De kwaliteit van de eenheidsauditors is divers. De centrale afdeling korpsaudit heeft veel aanvullende werkzaamheden moeten uitvoeren om het voor ons mogelijk te maken, te kunnen steunen op de werkzaamheden. Daarnaast hebben wij in afstemming met korpsaudit tevens aanvullende werkzaamheden moeten verrichten bij de betreffende eenheden.
- De reorganisatie waar de politie zich nu in bevindt vormt een continuïteitsrisico voor de borging van de Wpg, ook omdat de Wpg nu vooral op een aantal personen binnen de politie hangt. Tevens zien wij het risico dat wanneer het landelijke implementatietraject ophoudt met bestaan, de aandacht voor de Wpg verdwijnt.
- Ondanks de in de afgelopen periode ondernomen maatregelen, scoort de politie op de vijf risicogebieden overwegend rood. In opzet scoort de politie op de onderwerpen 'verstrekkingen', 'rechten van betrokkenen' en 'protocolplicht' groen. De overige twee onderwerpen, te weten: 'autorisaties' en 'bewaartermijnen' scoren in opzet rood. Daarnaast scoren alle vijf risicogebieden, zowel in bestaan als in werking, rood.
- Ten slotte zijn ook de zeven andere onderwerpen beoordeeld. Van deze onderwerpen scoren er drie rood, te weten 'kwaliteitsaspecten van politiegegevens', 'geautomatiseerd vergelijken en in combinatie verwerken' en 'in control werking alle onderdelen'. De overige vier, te weten 'gevoelige gegevens', 'ter beschikking stellen', 'privacyfunctionaris' en 'audits' scoren oranje.

1 Inleiding

1.1 Aanleiding

De Wet politiegegevens (Wpg) is op 1 januari 2008 van toepassing verklaard op de verwerking van politiegegevens door de politie.

De Wpg schrijft 'de verantwoordelijke' (voor de politie is dit de korpschef) voor om periodiek een privacy audit uit te laten voeren op de naleving van de regels die als gevolg van de Wpg van toepassing zijn op het verwerken van politiegegevens (artikel 33 lid 1). Tevens dient 'deze verantwoordelijke' tijdig opdracht te verstrekken aan een auditinstelling om de vierjaarlijkse privacy audit uit te voeren.

Een externe privacy audit dient de eerste keer na twee jaar en vervolgens na vier jaar plaats te vinden. Dit betekent dat eind 2010, eind 2014, eind 2018, eind 2022, en zo verder, een externe privacy audit uitgevoerd moet worden. De eerste externe privacy audit heeft plaatsgevonden in 2011 en is uitgevoerd door de voorloper van de ADR (de DAD van het ministerie van Veiligheid en Justitie).

De politie heeft de ADR de opdracht verstrekt een privacy audit over de periode 2011 t/m 2014 uit te voeren. De korpschef politie, dient een afschrift van het externe privacyrapport aan het College Bescherming Persoonsgegevens (CBP) te zenden.

De opdracht is beschreven in de opdrachtbrief, welke in april 2014 door de opdrachtgever, de heer D. Heerschop, en in mei 2014, door de opdrachtnemer van de ADR, de heer J. Looman, is ondertekend.

1.2 Uitvoering privacy audit

De privacy audit is uitgevoerd conform de richtlijnen (richtlijn 3600 van de NOREA) voor het uitvoeren van privacy audits van de Nederlandse Orde van EDP Auditors (NOREA).

Het onderzoek is gedaan volgens een door de ADR opgesteld werkprogramma. De uitgevoerde werkzaamheden bevatten onder meer: het beoordelen van de bevindingenmatrix en het auditdossier van de interne audit over 2011 t/m 2014, het houden van interviews onder medewerkers, het uitvoeren van deelwaarnemingen in de procesbeschrijvingen en andersoortige documentatie. De privacy audit heeft zich gericht op het verkrijgen van een redelijke mate van zekerheid ten aanzien van de hieronder genoemde doelstelling en objecten.

Het doel[1] van de privacy audit is op systematische wijze te toetsen of aan de bepalingen van de Wpg op adequate wijze uitvoering is gegeven.

Concreet betekent dit het beantwoorden van de vraag in hoeverre is geborgd dat voldaan wordt aan de bij of krachtens Wpg gestelde bepalingen, door de politie.

1 Conform artikel 2, lid 2 Regeling periodieke audit politiegegevens

Uit de hercontrole (die naar aanleiding van de eerste externe privacy audit is uitgevoerd) en uit de risicoanalyse (die in het voorjaar van 2013 door KPMG is uitgevoerd) is gebleken dat van de twaalf onderwerpen in de Wpg, er vijf onderwerpen waren, waar het korps het meeste risico loopt. Enerzijds omdat deze nog onvoldoende geïmplementeerd waren, anderzijds omdat dit onderwerpen zijn waarin het niet voldoen aan de Wpg de grootste impact heeft. Dit betreft de onderwerpen:

- autorisatie (art. 16)
- bewaartermijnen (art. 14)
- verstrekking (art. 16 t/m 24)
- rechten van betrokkene (art 25 t/m 31)
- protocolplicht (art 32).

In gesprekken tussen de politie en het CBP heeft het CBP aangegeven een volledige rapportage (over alle Wpg-aspecten) te verwachten van de ADR. Daarom is besloten de audit op de vijf risicovolle onderwerpen aan te vullen met een door korpscontrol uit te voeren statusupdate over de zeven andere Wpg-onderwerpen. De statusupdate is uitgevoerd in de vorm van een quickscan.

Voor de externe audit zal de ADR uitvoering geven aan de door de opdrachtgever, Dick Heerschop, verstrekte opdracht conform de hiervoor door NOREA (Nederlandse Organisatie van Register EDP Auditors) ontwikkelde norm. De ADR zal hierbij steunen op de werkzaamheden die door de interne auditors zijn uitgevoerd.

Door de vorming van de Nationale Politie bevindt de organisatie zich in een reorganisatiefase, waarin landelijke procedures, ook in het kader van de Wpg, worden opgezet. Als uitgangspunt voor de interne audit heeft men gekozen om hierbij aan te sluiten. Dit houdt in dat ook wij, als externe privacy auditor, uitgaan van de landelijke procedurebeschrijvingen bij de uitvoering van de audit.

Het conceptrapport is op 15 oktober 2015 besproken met de politie.

1.3 Doelgroep van het rapport

Het rapport wordt aangeboden aan onze opdrachtgever, de heer D. Heerschop, lid Korpsleiding en CIO, die voor verdere verspreiding zorg draagt.

1.4 Leeswijzer

In hoofdstuk 2 beschrijven wij de bevindingen vanuit de privacy audit. In paragraaf 2.1 wordt ingegaan op de algemene bevindingen, waarna wij in paragraaf 2.2 de bevindingen per Wpg onderwerp presenteren.

2 Bevindingen

2.1 Algemene Bevindingen

De eenheden hebben de afgelopen periode werkzaamheden verricht in het kader van het implementatietraject van de Wpg. Hierdoor is de bewustwording van de Wpg groeiende en wordt het belang en nut van de Wpg vaker onderkend, met name in vergelijking met de eerste privacy audit. Binnen het implementatietraject heeft men landelijke procedures opgezet voor een aantal risicovolle Wpg-onderwerpen. Omdat deze landelijke procedures (nog) niet juist en volledig zijn geïmplementeerd, worden nog veelal de eenheidsprocedures gehanteerd. Aan het bestaan van de Wpg wordt momenteel invulling gegeven door de landelijke- en eenheidsprocedurebeschrijvingen te vertalen naar werkinstructies, gerichte opleidingen voor het personeel, functiebeschrijvingen en roltoebedelingen. Doordat de implementatie van de landelijke procedures binnen de eenheden nog niet is afgerond en er binnen de politie verschillende werkwijzen bestaan, scoort men een onvoldoende op bestaan en werking.

De conclusie is dat de politie niet of niet geheel voldoet aan de Wpg. In 2008 had de Wpg echter al binnen de politieorganisatie geïmplementeerd moeten zijn. De grootste oorzaak hiervan lijkt te zijn dat de Wpg binnen de politie wordt gezien als een 'losstaand project' , terwijl dit onderdeel uit zou moeten maken van alle politieprocessen. Tegelijkertijd ondersteunen de IT-systemen de gebruikers onvoldoende, waardoor onevenredig veel inspanning is vereist om buiten de systemen om, de Wpg normen na te kunnen leven. Zo zijn in de IT-systemen de geautomatiseerde controles voor de Wpg niet ingebouwd en is het autorisatie- en gegevensbeheer nog niet op orde. Hierdoor vormen onder andere de autorisaties en bewaartermijnen een groot risico voor de bescherming van de privacy en ongeoorloofde toegang tot politiegegevens.

Toelichting context
De afdeling korpsaudit is verantwoordelijk voor de interne audits voor de Wpg. Daarnaast zijn binnen de eenheden auditors aangewezen die de werkzaamheden uitvoeren voor de interne audit. Wij hebben vastgesteld dat de kwaliteit van de eenheidsauditors divers is. Hoewel de kennis op het gebied van politieprocessen en Wpg voldoende aanwezig is, ontbreekt specifieke auditervaring en opleiding en is de onafhankelijkheid onvoldoende geborgd. De centrale afdeling korpsaudit heeft veel aanvullende werkzaamheden moeten uitvoeren om het voor ons mogelijk te maken, te kunnen steunen op de werkzaamheden. Daarnaast hebben wij in afstemming met korpsaudit aanvullende werkzaamheden moeten verrichten bij de betreffende eenheden.

Daarnaast bevindt de politie zich nu in een reorganisatiefase. Dit zorgt ervoor dat veel personeel nu nog niet op de juiste plek zit (ook bij korpsaudit) en dat de komende periode nog de nodige verschuivingen plaats zullen vinden. Dit vormt een continuïteitsrisico voor de borging van de Wpg, ook omdat de Wpg nu vooral op een aantal personen binnen de politie hangt. Tevens zien wij het risico dat wanneer het landelijk implementatietraject ophoudt met bestaan, de aandacht voor de Wpg verdwijnt.

2.2 Bevindingen per Wpg onderwerp

Ten eerste worden in onderstaande tabel de vijf onderwerpen behandeld welke zijn geïdentificeerd als risicothema's. Voor deze vijf onderwerpen is de opzet (landelijke procedure is opgesteld), het bestaan (landelijke procedure is geïmplementeerd) en de werking (over bepaalde periode wordt gewerkt conform Wpg) beoordeeld.
Voor de zeven andere onderwerpen is in de tweede tabel vastgesteld of maatregelen zijn genomen ter verdere verbetering van de status zoals vastgesteld in de rapportage 'hercontrole audit Wpg 2013'. Dit betreft een score op de werking.

De bevindingen zijn verwerkt in een matrix waarbij in kleur de scores zijn aangegeven van de beoordeling van de opzet (O), het bestaan (B) en de werking (W). Daarbij hebben we de volgende criteria gehanteerd:

Groen: er wordt in hoofdlijnen voldaan aan de norm.
Oranje: er wordt niet of niet geheel voldaan aan de norm.
Rood: er wordt niet voldaan aan de norm.
Grijs: niet vast te stellen of niet van toepassing.

Wpg onderwerp	Bevindingen	Score		
		O	B	W
Autorisaties Autorisaties aanvragen en wijzigingen (proces) Autorisaties intrekken(proces) Inrichting van het autorisatiesysteem (kader) Controle en toezicht op het proces en het systeem Ingerichte autorisaties in IT systemen	Er is nog geen landelijke procedure voor autorisaties opgesteld. De meeste eenheden hebben inmiddels autorisatieloketten opgezet, echter de medewerkers zijn hier nog vaak onbekend mee. Het autorisatieproces is daarmee onvoldoende op orde. Het aanvragen van autorisaties wordt heel divers ingevuld door de eenheden, middels eigen vaste procedures. Slechts bij één van de eenheden is een procedure aangetroffen voor het intrekken van autorisaties. Ook ontbreken regelmatig de autorisatiematrixen en/of zijn deze niet actueel. Ten slotte worden er geen gestructureerde controles uitgevoerd op autorisaties.			
Verstrekken art. 16-verstrekking aan opsporingsambtenaren en gezagsdragers art. 17/24-verstrekking aan inlichtingendiensten en buitenlandse opsporingsinstanties art. 18-verstrekking aan derden structureel art. 19-verstrekking aan derden incidenteel art. 20-verstrekking aan derden structureel voor samenwerkings verbanden art. 22-verstrekking voor wetenschappelijk onderzoek en statistiek	Er is een landelijke procedure voor verstrekkingen opgesteld. Deze is echter nog niet (volledig) binnen alle eenheden geïmplementeerd. Niet elk type verstrekking voldoet aan de Wpg. Dit geldt bijvoorbeeld voor die aan de burgemeesters en BOA's, waar nog onvoldoende invulling wordt gegeven aan het noodzakelijkheids-, proportionaliteits- en subsidiariteitsbeginsel. Bij steeds meer eenheden zijn convenantenloketten opgezet.			
Protocolleren vastleggen doel verwerkingen, (art 9 lid 2) art.32,1A vastleggen van een verwerking als bedoeld in artikel 13 lid 4 verwerking (art 32,1B) Protocolleren van de toekenning van autorisaties.(art.32,1C)	Er is een landelijke procedure protocolplicht opgesteld. Deze is echter nog niet (volledig) binnen alle eenheden geïmplementeerd. Voor alle categorieën waarvoor geprotocolleerd dient te worden gebeurt dit nog niet conform de Wpg.			

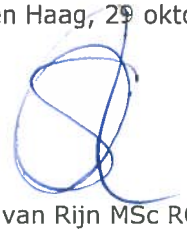
Protocolleren van geautomatiseerde vergelijking/combinatie verwerken (art.32,1D) Protocolleren hernieuwde verwerking (art.32,1E) Protocolleren van verstrekkingen.(art.32,1F) Protocolleren onrechtmatige verwerkingen (art.32,1G) Protocolleren van geautomatiseerde vergelijkingen van politiegegevens met andere dan politiegegevens.(art.32,1H)				
Bewaartermijnen Verwerken politiegegevens dagelijkse politietaak (art.8) Verwerken van politiegegevens t.b.v een onderzoek in een bepaald geval (art.9) Verwerken van politiegegevens ivm inzicht van de betrokkenheid van personen bij ernstige bedreiging rechtsorde.(art.10) Verwerken politiegegevens ivm informantenbeheer (art.12) Verwerken politiegegevens tbv ondersteunende taken (art.13) Verwerken politiegegevens tbv klachten, verantwoording, rechten v. betrokkene en hernieuwde verwerking (art.14)	De bewaartermijnen zijn onvoldoende op orde. Dit komt mede omdat deze niet zijn geborgd in de IT. De medewerkers dienen zelf schoningstermijnen in de gaten te houden en handmatig te schonen. Dit gebeurt meestal niet.			
Rechten van de betrokkene Verzoek tot kennisneming (art 25-27) Verzoek om verbetering, aanvulling, verwijdering of afscherming Vergoeding van kosten Overige	Er is een landelijke procedure voor rechten van betrokkenen opgesteld, echter is deze nog niet binnen alle eenheden geïmplementeerd. De processtappen zoals kennisneming en verzoek om verbetering, aanvulling, verwijdering of afscherming zijn op dit moment nog onvoldoende op orde en voldoen daarmee niet aan de Wpg-eisen. De politie brengt geen kosten in rekening.			

Wpg onderwerp	Bevindingen	Score Werking
Kwaliteits-aspecten van politie-gegevens	In alle eenheden wordt True Blue gebruikt als tool voor kwaliteitsverbetering. De kennisregels zijn echter nog te beperkt en de naleving van alerteringen is niet optimaal, waardoor dit onderwerp nog niet op orde is.	
Gevoelige gegevens	De landelijke richtlijnen zoals verwoord in het Praktijkhandboek Wpg en de instructies voor de bevoegd functionaris worden gevolgd. Er worden in de eenheden wel gevoelige gegevens vastgelegd, maar dit is vrijwel altijd in relatie tot bijvoorbeeld de aanpak van criminele groepen. Er worden ten aanzien van gevoelige gegevens ook opleidingen gevolgd. In de grote steden wordt aangegeven dat omgaan met andere etniciteiten als normaal wordt beschouwd. Desondanks is uit de audit naar voren gekomen dat op dit punt nog verdere verbetering mogelijk is.	
Geautomati-seerd vergelijken en in combinatie verwerken	Binnen de politie is een aantal medewerkers belast met werkzaamheden van geautomatiseerd vergelijken en in combinatie met elkaar verwerken binnen artikel 9 en 10 verwerkingen. Vaak zijn deze informatiecoördinatoren niet aangewezen in deze tijd van reorganiseren. Zo is niet geborgd dat in combinatie met elkaar verwerken van artikel 8 politiegegevens ouder dan 1 jaar door de informatiecoördinator moet gebeuren.	
Ter beschikking stellen	De meeste executieve medewerkers hebben de tool BVI-IB ter beschikking gesteld gekregen. Hiermee kunnen online op straat de meest voorkomende systemen met artikel 8- en 13.1-gegevens worden geraadpleegd voor de uitvoering van de dagelijkse politietaak. Voor wat betreft de overige gegevens blijkt dat bevoegd functionarissen vaak te weining informatie over hun onderzoek willen delen met collega's buiten hun team. Op basis van de interviews stellen wij vast dat er binnen de eenheden nog geen uniform beleid is met betrekking tot het aanstellen en opleiden van bevoegd functionarissen. Bevoegd functionarissen weten niet welke verantwoordelijkheden en bevoegdheden zij hebben en handelen dus niet daarnaar.	

Audits	De afdeling korpsaudit is verantwoordelijk voor de interne audits ten behoeve van de Wpg. Daarnaast zijn binnen de eenheden interne auditors aangewezen die de werkzaamheden uitvoeren voor de interne audit. Wij hebben vastgesteld dat de kwaliteit van de eenheidsauditors divers is. Hoewel de kennis op het gebied van politieprocessen en Wpg voldoende aanwezig is, ontbreekt de specifieke auditervaring en opleiding en is de onafhankelijkheid onvoldoende geborgd. De centrale afdeling korpsaudit heeft veel aanvullende werkzaamheden uitgevoerd waardoor het uiteindelijk voor ons mogelijk was om te steunen op de uitgevoerde werkzaamheden.	
Privacy-functionaris	Alle eenheden hebben de beschikking over één of meerdere privacyfunctionarissen. Echter de capaciteit is in een aantal eenheden onvoldoende. Slechts een aantal privacyfunctionarissen houdt op eigen initiatief, veelal beperkt, toezicht. In het verleden is er bij een aantal oud korpsen wel toezicht uitgeoefend en controles gehouden.	
In control werking alle onderdelen	Er vindt weinig actieve sturing plaats op het onderwerp Wpg. De Wpg krijgt in het totaal van prioriteiten niet altijd voldoende aandacht. In een aantal eenheden staat de Wpg wel met enige regelmaat op de agenda van het eenheidsleidingsoverleg (ELO). Bij opsporing en bij informatie-onderdelen is over het algemeen meer sturing, kennis en interesse voor de Wpg aanwezig. Het merendeel van de geïnterviewden geeft aan dat er een vorm van controle van het werk van de medewerker is. Soms in de vorm van collegiale toetsing, soms wordt de controle door de leidinggevende uitgevoerd en dan vaak steekproefsgewijs. Een aantal geïnterviewden geeft aan dat controle op hun werk gemist wordt. Er is nog niet voldoende managementinformatie beschikbaar om te kunnen bijsturen. Er vindt kortom onvoldoende monitoring en (bij)sturing plaats.	

3 Ondertekening

Den Haag, 29 oktober 2015



S. van Rijn MSc RO
Senior auditor

Auditdienst Rijk
Postbus 20201
2500 EE Den Haag
(070) 342 77 00